UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,777	12/12/2000	Antonius A.M. Staring	PHN 17,813	4699

24737 7590 05/06/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	4

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/734,777	STARING, ANTONIUS A.M.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-7 and 9-12* is/are rejected.

7)☒ Claim(s) *3,8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2000* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 99/204182.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: On page 9 line 28, the number "4" should be inserted after "figure".

Appropriate correction is required.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "232" has been used to designate both KCB_N and KCB_{N+1}. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims ~~1-12~~ 1,2,4-7, and 9-12 rejected under 35 U.S.C. 103(a) as being unpatentable over Komuro et al (US pat 6,223,285), and further in view of Gray et al (US pat 5,706,348).

Regarding claim 1, Komuro et al teach A secure communication system including a source device and at least one sink device; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information;

the source device including:

a key generator for, at the initiative of the source device, generating an active source session key (col.9 lines 22-28);

an encryptor for encrypting at least part of the data field of a packet under control of the active source session key (col.9 lines 28-32);

the sink device including:

a key generator for generating a plurality of candidate sink session keys, where for each index in the sequence the respective sink session key corresponds to the respective source session key (col.10 lines 18-22);

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key (col.10 lines 22-27);

a key resolver (col.10 lines 16-18) operative to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, and to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key (col.10 lines 22-27).

What Gray et al teach that Komuro et al do not teach is:

generating session keys in a predetermined sequence (col.2 lines 35-36);

the encrypted part of the data field including a sub-field designated as a key check block field (col.5 lines 55-64);

by causing the decryptor to decrypt the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found (col.5 line 65 thru col.6 line 27). It would have been obvious to one of ordinary skill in the art to combine Komuro et al's system of transferring information using an encryption mode indicator with Gray et al's method of updating and checking keys periodically in order to enhance security by preventing data security risks (Gray et al col.2 lines 35-36; col.2 lines 47-51).

Regarding claim 2, Komuro et al and Gray et al teach a secure communication system as claimed in claim 1, in addition Gray et al teach the plain-text form of the key check block in the key check block field is a public data block (col.5 lines 55-64).

Regarding claim 4, Komuro et al and Gray et al teach a secure communication system as claimed in claim 1, in addition Gray et al teach the plain-text form of the key check block in the key check block field changes at least once during the communication session (col.2 line 35-36; col.2 lines 58-60).

Regarding claim 5, Komuro et al and Gray et al teach a secure communication system as claimed in claim 4, in addition Gray et al teach the source and sink device include corresponding key check block generators for generating the plain-text form of the key check block and effecting the change of the plain-text form of the key check block (col.4 lines 41-59; col.5 lines 55-64).

Regarding claim 6, Komuro et al and Gray et al teach a secure communication system as claimed in claim 4, in addition Gray et al teach the plain-text form of the key check block of a particular packet is derived from information transferred in a packet preceding the particular packet (col.5 lines 7-13; col.5 lines 40-64).

Regarding claim 7, Komuro et al and Gray et al teach a secure communication system as claimed in claim 4, in addition Gray et al teach the plain-text form of the key check block is derived from information transferred in a packet immediately preceding the particular packet (col.5 lines 14-17; col.5 lines 55-64).

Claims 9-12 are substantially equivalent to claim 1, therefore claims 9-12 are rejected because of similar rationale.

Allowable Subject Matter

5. Claims 3 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of

the base claim and any intervening claims. The following is a statement of reasons for the indication of allowable subject matter:

With respect to claim 3, the cited prior art fails to specifically teach a secure communication system as claimed in claim 1, wherein the plain-text form of the key check block in the key check block field is a data block agreed between the source and sink device before starting the transfer of the information and used for the entire communication session.

With respect to claim 8, the cited prior art fails to specifically teach a secure communication system as claimed in claim 6, wherein the plaintext form of the key check block of a particular packet is identical to the plain-text form of a predetermined data block, other than the key check block, in an encrypted part of the data field of a packet preceding the particular packet.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

April 19, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137